



Data Breach Response Plan

Legal name:

ALL ABOUT CARE AUSTRALIA PTY LTD

Business/trading name:

AACA

ABN: 30 650 354 144

ACN: 650 354 144

Primary address/head office: 3 Cockatiel Court Loganlea QLD 4131

NDIS Registration ID: 4-G6H3XZP

Table of Contents

1. Introduction

- 1.1. Purpose of the data breach response*
- 1.2. What is a data breach?*
- 1.3. What is an eligible data breach*

2. Responsibilities and process for data breaches

- 2.1. Contain*
- 2.2. Assess*
- 2.3. Manage and Notify*
 - 2.3.1. Remedial action*
 - 2.3.2. Notification*
- 2.4. Review*
 - 2.4.1. Circumstances in which other relevant bodies may need to be contacted*

3. Data breach response team roles and responsibilities

4. Records management, reporting, and review.

- 4.1. Records management*
- 4.2. Reporting*
- 4.3. Review of the Plan*

5. References and related content

- 5.1. References*
- 5.2. Related Content*

1 Introduction

1.1 Purpose of the Data Breach Response

This data breach response plan (the Plan) details the necessary steps that should be taken if AACA experiences a data breach (or suspects that a data breach has occurred). The Plan outlines the roles and responsibilities of staff (including staff who are employed and those engaged under a contract) and documents the process that should be followed to enable AACA to contain, assess and quickly respond to a data breach to help mitigate potential harm to affected individuals.

Together with AACA's Privacy Policy and other associated policies, this Plan will enable AACA to comply with the notifiable data breaches (NDB) scheme that commenced on 22 February 2018. The Plan will enable AACA to effectively manage and limit the consequences of a data breach on affected individuals, reduce the costs associated with dealing with a breach, and reduce the potential reputational damage that can result.

A data breach covered by the NDB scheme occurs when personal information is lost or subjected to unauthorised access or disclosure. For good privacy practice purposes, this Plan also covers any instances of unauthorised use, modification, or interference with personal information held by AACA.

1.2 What is a Data Breach?

A data breach occurs when personal information held by AACA is lost or subjected to unauthorised access or disclosure. For simplicity, this policy refers to data breaches of 'personal information', but it applies to all information held by AACA (including any information about an individual's tax file number).

A data breach may be caused by malicious action (by an external or insider party), human error, or a failure in information handling or security systems.

Examples of how a data breach could occur include:

- loss or theft of physical electronic devices (such as laptops and storage devices) or paper records that contain personal information
- unauthorised access to personal information by an employee or external party
- inadvertent disclosure of personal information due to 'human error', for example, an email sent to the wrong person
- disclosure of an individual's personal information to a malicious party (e.g. a scammer, an activist, a disgruntled ex-employee, or an estranged family member), as a result of inadequate identity verification procedures.

Data breaches can be caused or exacerbated by a variety of factors, affect different types of personal information, and give rise to a range of actual or potential harms to affected individuals.

Individuals whose personal information is involved in a data breach may be at risk of serious harm, whether that is harm to their physical or mental well-being, financial loss, or damage to their reputation.

Examples of harm include:

- financial loss including unauthorised credit card transactions or credit fraud
- identity theft causing financial loss or emotional and psychological harm

- family violence
- physical harm, bullying or intimidation
- loss of business or employment opportunities
- humiliation/damage to reputation or relationships.

A data breach can also negatively impact AACA's reputation for privacy protection, and as a result may undercut its commercial interests and industry standing.

1.3 What is an Eligible Data Breach

The Notifiable Data Breaches (NDB) scheme requires AACA to notify affected individuals and the Australian Information Commissioner about 'eligible data breaches.' This notification allows affected individuals to take the required steps to reduce or remove the risk of harm.

An 'eligible data breach' will occur under the Privacy Act when the following three criteria are satisfied:

- there is unauthorised access to or unauthorised disclosure of personal information that AACA holds, or there is a loss of personal information in circumstances where unauthorised access or disclosure of the information is likely; and
- this is likely to result in serious harm to one or more individuals to whom the personal information relates; and
- no exception in the Privacy Act applies. The most likely exception in most cases will be that AACA has taken remedial action which has prevented the likely risk of serious harm occurring.

If it is not clear whether a suspected data breach meets these criteria, an objective assessment, determined from the viewpoint of a reasonable person within AACA, must be completed to determine whether the breach is an 'eligible data breach' that triggers notification obligations. Not all data breaches will be 'eligible data breaches.' For example, if AACA acts quickly to remediate a data breach, and as a result of this action the data breach is not likely to result in serious harm, the exception in the Privacy Act will apply and there will be no requirement to notify any affected individuals or the Commissioner under the NDB scheme.

For more information on what constitutes an 'eligible data breach', see the OAIC guide '*Data Breach Preparation and Response*'.

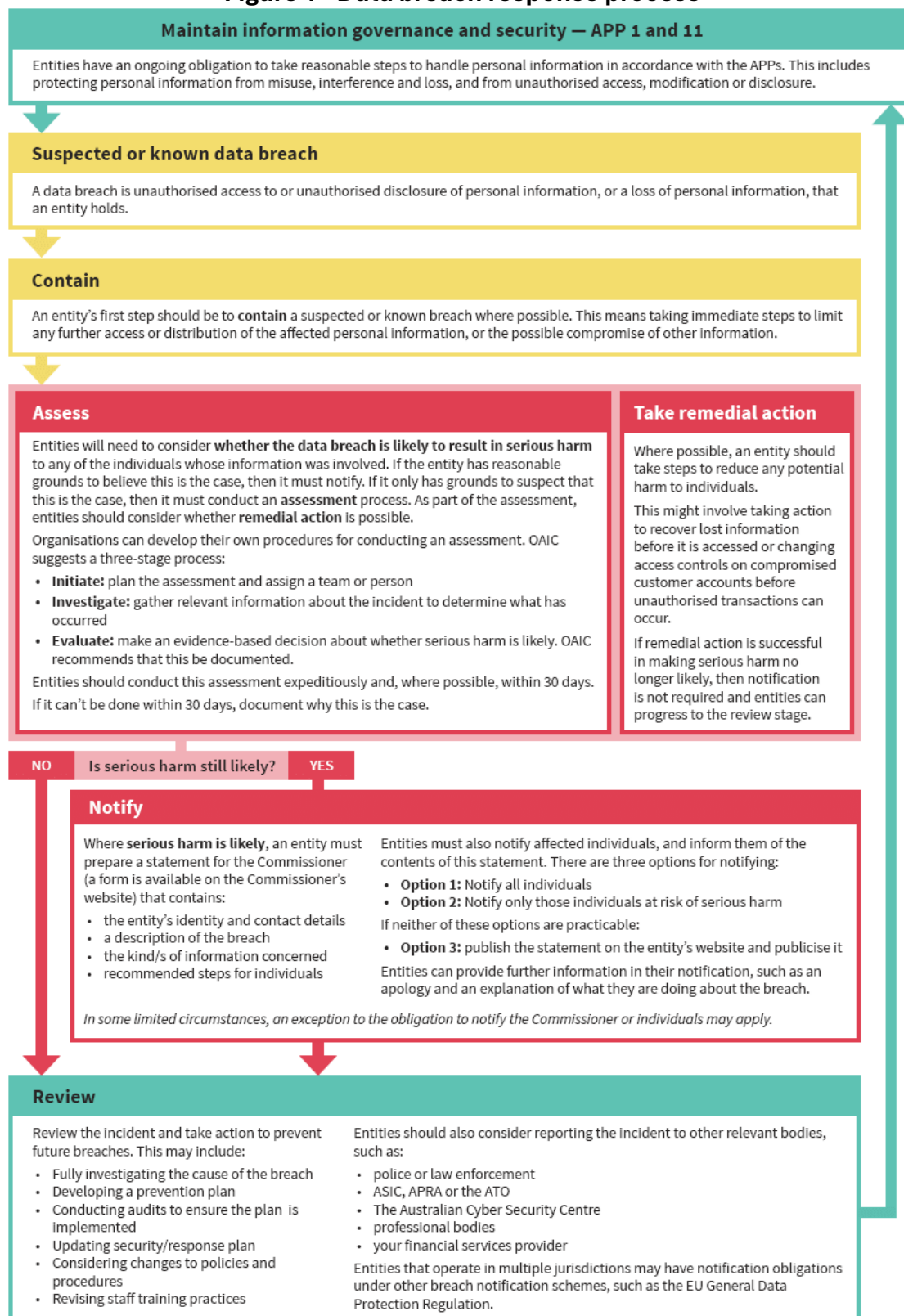
2 Responsibilities and process for data breaches

Broadly AACA will take a Contain-Assess-Manage-Review approach to data breaches as detailed in Figure 1. AACA process and responsibilities for enabling this approach are summarised in Figure 2 and have been outlined in further detail within section 2.

Note: There is no single method of responding to a data breach. Data breaches must be dealt with on a case-by-case basis by undertaking an assessment of the risks involved and using that risk assessment to decide the appropriate course of action. Depending on the nature of the breach, additional staff or external experts may need to be included, for example an IT specialist/data forensics expert or a human resources adviser.

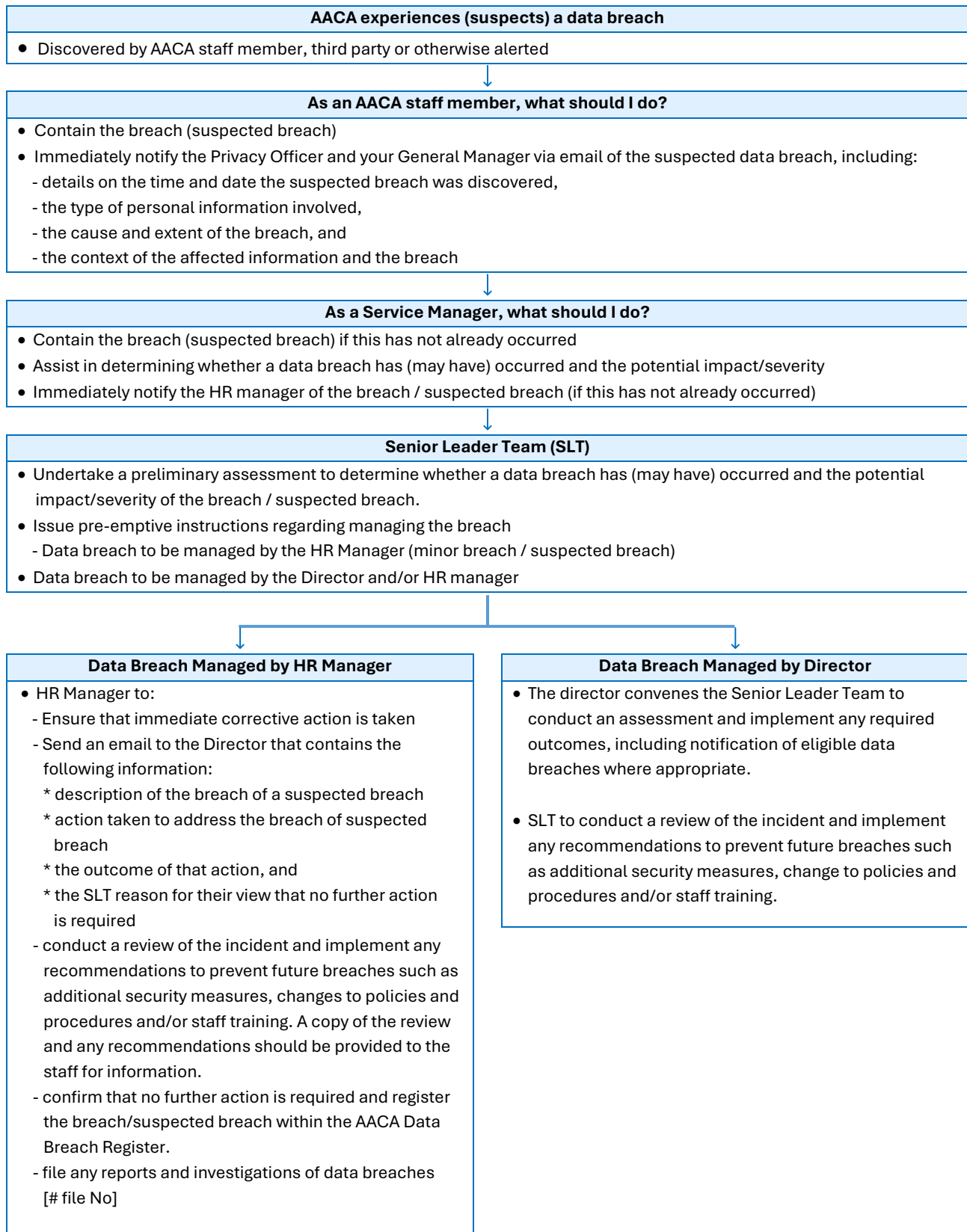
The AACA Data Breach Response Team is responsible for carrying out the actions that can reduce the potential impact of a data breach, however individual AACA staff are responsible for notifying the Service Manager and HR Manager of a suspected or confirmed data breach as soon as they become aware of the breach.

Figure 1 - Data breach response process



- Source: Office of the Australian Information Commissioner (OAIC)

Figure 2 - AACCA process for responding to a data breach (suspected breach)



2.1 Report and Contain

Reporting

If a staff member discovers or is otherwise alerted to, a data breach or a suspected data breach, the first step is for the staff member to immediately report the data breach to the Service Manager or HR Manager. This may be done orally but should be followed up with a written notice (by email) within 24 hours.

The email should include the following details:

- the time and date the suspected/known breach was discovered,
- the type of personal information involved,
- the cause and extent of the breach, and
- the context of the affected information and the breach.

If an external contractor reports an actual or suspected data breach, the relevant contract should be reviewed to determine what action is to be taken. AACA may be able to:

- participate in the contractor's assessment of the event and whether it amounts to an eligible data breach; and
- meet with the contractor to discuss and agree who will issue any required notification.

Containing the impact

The Service Manager or HR Manager will assist the staff member to contain a suspected or known breach where possible. This means taking immediate steps to limit any further access or distribution of the affected personal information, or the possible compromise of other information.

The containment should be done by, to the extent practical and possible, the staff member who first suspects or is made aware of the data breach.

What is needed to contain the breach is determined on a case-by-case basis, however, addressing the following questions may help to identify strategies to contain a data breach:

- How did the data breach occur?
- Is the personal information still being shared, disclosed, or lost without an authorisation?
- Who has access to the personal information?
- What can be done to secure the information, or stop the unauthorised access or disclosure, and reduce the risk of harm to affected individuals?

All staff should be careful not to destroy evidence that may be valuable in identifying the cause of the breach, or that would enable AACA to address all risks posed to affected individuals or AACA.

2.2 Assess

The Service Manager is responsible for undertaking a preliminary assessment of whether an eligible data breach has or may have occurred, and the impact and severity of that actual or suspected breach.

If the Service Manager is satisfied that no eligible data breach has occurred, the Service Manager must confirm this with the HR Manager. The HR Manager agrees with the conclusion, the Supervisor will document and file their reasons for this conclusion, and no further action will be taken.

If after undertaking this initial assessment, the Service Manager is of the view that a data breach has, or may have, occurred, the Service Manager must either:

- Where the Service Manager is of the view that the risks associated with any data breach are low, and that remedial action can be appropriately taken so that the incident will not be an eligible data breach – ensure the remedial action is taken by the HR Manager. For example, an AACA employee may, as a result of human error, send an email containing personal information to the wrong recipient. Depending on the sensitivity of the contents of the email, if the email can be successfully recalled (only relates to internal emails), or if the officer can contact the recipient and obtain an assurance that the recipient has deleted the email, this will no longer be an eligible data breach. There is no need to escalate the issue to the Director.
- Otherwise, the HR Manager must refer the matter to the Senior Leader Team (SLT).

In conducting their initial assessment, the Service Manager should consider

- whether any individual may be “at risk” of serious harm now or in the future (this will require the Service Manager (and the SLT if the matter is escalated to it) and consider a wide variety of factors such as the sensitivity of the information, whether the information is protected by one or more security measures, the kind of person(s) who could obtain the information and the nature of the harm)
- the number of people affected by the breach or suspected breach
- the type of personal information involved in the data breach
- circumstances of the data breach, including its cause and extent
- the nature of the harm, and whether this can be removed through remedial action
- whether the data breach or suspected data breach may indicate a systemic problem with AACA's practices or procedures
- other issues relevant to the circumstances, such as the value of the data to AACA or issues of reputational risk.

If the Service Manager escalates the matter to the SLT, the SLT must conduct an assessment to determine whether the incident amounts to an eligible data breach (as defined in the Privacy Act). This assessment process must be completed within 30 calendar days of the day AACA becomes aware of the grounds (or information) that caused AACA to suspect an eligible data breach. The Australian Information Commissioner expects that wherever possible entities treat 30 days as a maximum time limit for completing an assessment, and endeavour to complete the assessment in a much shorter timeframe, as the risk of serious harm to individuals often increases with time.

The SLT's assessment should follow the below three-phase process:

1. **Initiate:** Plan the assessment and assign a team or person
2. **Investigate:** Gather relevant information about the incident to determine what has occurred
This will involve gathering together all necessary and relevant information about the actual or suspected data breach. It should include a prompt initial assessment of the following:

- What information has been lost or accessed or disclosed without authorisation?
- What was the cause of the data breach?
- What is the extent of the data breach?
- What individuals have been, or may be, affected by the data breach, and the extent of the harm?
- Are there ways that the data breach can be contained (as it is vital to ensure as quickly as possible that there are not ongoing or repeated data breaches stemming from the same or related causes)?
- Is there any need to immediately notify any person potentially affected (and if so, who and what information should be disclosed to them)?

Evidence may be needed later to find the cause of the problem or to fix the issue, so care needs to be taken to ensure that nothing is destroyed.

The SLT may seek internal or external advice to assist it as required.

3. Evaluate: Make an evidence-based decision about whether serious harm is likely or whether any exception to notification in the Privacy Act applies, and document this decision.

Where AACA cannot reasonably complete an assessment within 30 days, this should be documented so that AACA can demonstrate:

- that all reasonable steps have been taken to complete the assessment within 30 calendar days
- the reasons for the delay
- that the assessment was reasonable and expeditious.

If the SLT determines that the incident was an eligible data breach (as defined in the Privacy Act) then AACA must notify the affected individuals and Australian Information Commissioner as per section 2.3.

There are exceptions to notifying in certain circumstances. The SLT will assess whether an exception is applicable to the situation.

2.3 Manage and Notify

2.3.1 Remedial action

Where possible, AACA will promptly take steps to reduce any potential harm to individuals. This might involve taking action to recover lost information before it is accessed or changing access controls on compromised stakeholder accounts before unauthorised transactions can occur. It may also involve any compromised security credentials being revoked, and affected by a virus or malware being isolated or turned off.

If remedial action is successful in preventing the likelihood of serious harm, then notification is not required and the SLT can progress to the review stage.

2.3.2 Notification

If the SLT determines that there has been an eligible data breach, the HR Manager will prepare a statement for the Commissioner using the Notifiable **Data Breach Statement — Form**, which will contain the following:

- AACCA's contact details
- a description of the breach
- the kind/s of information concerned
- recommended steps for individuals.

A nominated representative (determined by the SLT) will also notify affected individuals and inform them of the contents of this statement. The SLT will determine which of the following three options will be used for this notification:

- **Option 1:** Notify all affected individuals (where AACCA cannot reasonably assess which particular individuals are at risk of serious harm from an eligible data breach that involves personal information about many people, but where AACCA has formed the view that serious harm is likely for one or more of the individuals)
- **Option 2:** Notify only those individuals at risk of serious harm (where AACCA can identify that only a particular individual, or a specific subset of individuals, involved in an eligible data breach is at risk of serious harm, and can specifically identify those individuals)
- **Option 3:** publish the statement on AACCA website and publicise it (where neither of the first two options are practicable).

Where appropriate, the DBRT will provide further information in the notification, such as an apology and a summary of actions taken regarding the breach.

There are some exceptions to the notification requirements, which relate to:

- eligible data breaches of other entities
- enforcement related activities
- inconsistency with secrecy provisions
- declarations by the SLT

Where applicable, the SLT will consider any applicable exceptions, and refer as required to the guidance provided on the Office of the Australian Commissioner website.

Each data breach needs to be considered on a case-by-case basis to determine whether notification is mandatory or desirable (even if notification is not legally required, there may be reasons why AACCA may decide to issue a notification).

2.4 Review

Once notification obligations are completed, the SLT will meet to review the incident and take action to prevent future breaches. This may include:

- fully investigating the cause of the breach
- developing a prevention plan
- conducting audits to ensure the plan is implemented
- updating the security/response plan

- considering changes to policies and procedures
- revising staff training practices.

The SLT will also review and assess the data breach response and the effectiveness of this Data Breach Response Plan, including:

- whether the data breach or suspected data breach may indicate a systemic problem with AACA practices or procedures
- possible motives for the breach (where intentional)
- other relevant issues, such as the value of the data to AACA or issues of reputational risk.

2.4.1 Circumstances in which other relevant bodies may need to be contacted

Where relevant, a nominated representative of AACA's executive team may also report the incident to other relevant bodies, such as:

- police or law enforcement (where the breach may lead to fraud, violence or other illegal acts)\
- Australian Securities and Investments Commission (ASIC), Australian Prudential Regulation Authority (APRA) or the Australian Taxation Office (ATO), (where the breach may lead to fraud, or where financial information is involved)
- the Australian Cyber Security Centre (where the breach is in the form of a cyber-attack)
- AACA financial services providers (where AACA financial systems have been compromised)
- AACA's insurer(s)
- co-holders of personal information (where information is stored on a shared database)
- other third parties as appropriate (where required under agreements with third parties such as insurance policies or service agreements)
- in the event that a data breach was caused by a staff member, AACA's HR department will be notified (so they can ensure appropriate training at a minimum)

3 Senior Leader Team roles and responsibilities

The SLT should meet annually to review and assess this Data Breach Response Plan and make any necessary adjustments. The membership and responsibilities of the SLT include:

- Service Manager/ HR Manager
 - ensure appropriate actions are taken when required
 - report to the Executive Team
 - ensure AACA compliance with relevant policies and guidelines
 - advise on likely risk and/or harm
 - advise on mitigation measures
 - publish data breach notifications where necessary
- Director
 - provide legal advice
 - advise on likely risk and/or harm
 - provide communication/public relations/reputation management advice and support
 - provide information and records management advice and expertise

Depending on the nature of the breach the SLT may require additional expertise from members of Human Resources, Finance or other business areas. This will be determined as part of the assessment phase. In the case where a nominated member of the DBRT is involved in the breach or is unavailable, another representative from the required business area should be appointed.

Once a matter has been escalated to the SLT, the process outlined in Section 2 of the Data Breach Response Plan must be followed. The SLT must work in consultation with the Executive in responding to the breach. Each breach will need to be dealt with on a case-by-case basis, undertaking an assessment of the risks involved and using that risk assessment as the basis for deciding what actions to take in the circumstances.

4 Records management, reporting and review

4.1 Records management

Any documents created by the Privacy Officer and the SLT relating to a data breach (or suspected breach) should be saved in the relevant record keeping system. This includes post-breach and testing reviews, notifications and AACCA's Data Breach Register.

4.2 Reporting

The internal handling of personal information will be an agenda item on the Audit and General Staff Meeting at least once each quarter and include a report of any privacy complaints against AACCA and internal data breaches (or suspected breaches).

4.3 Review of the Plan

This Plan will be reviewed regularly (at least once every two years) to ensure that it is up to date. AACCA will also run drills of the procedures outlined in this Plan.

5 References and related content

5.1 References

This Plan has been developed in accordance with and with reference to the:

- *Privacy Act 1988 (Cth)*
- AACCA's Privacy Policy
- OAIC's *Data breach preparation and response - A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)*
- OAIC's *Guide to securing personal information - 'Reasonable steps' to protect personal information*

In the event of a data breach, the Privacy Officer and DBRT should reference the OAIC's Guide to securing personal information as it provides further detail that may be of assistance.

5.2 Related Content

- AACCA Privacy Policy
- AACCA Code of Conduct
- Information Security Policy
- Feedback and Complaint & Resolution

PROCEDURE INFORMATION	
Accountable Officer	Director, HR Manager, Service Manager
Approved Date	
Review Date	
Issue of Reporting	
Recorded History	

DISCLAIMER: This document is for internal use only and contains confidential and proprietary information. Once printed, this document becomes an uncontrolled copy and is current as at the date of printing. Version control and quality control cannot be guaranteed once downloaded from AACCA Intranet. For the most up-to-date version, please refer to AACCA Intranet.